PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G11B 20/00, G06F 1/00

A1

(11) International Publication Number: WO 00/67256

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/EP00/03801

(22) International Filing Date: 27 April 2000 (27.04.00)

(30) Priority Data:

60/131,993	30 April 1999 (30.04.99)	US
09/548,728	13 April 2000 (13.04.00)	US

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor: EPSTEIN, Michael, A.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: GROENENDAAL, Antonius, W., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

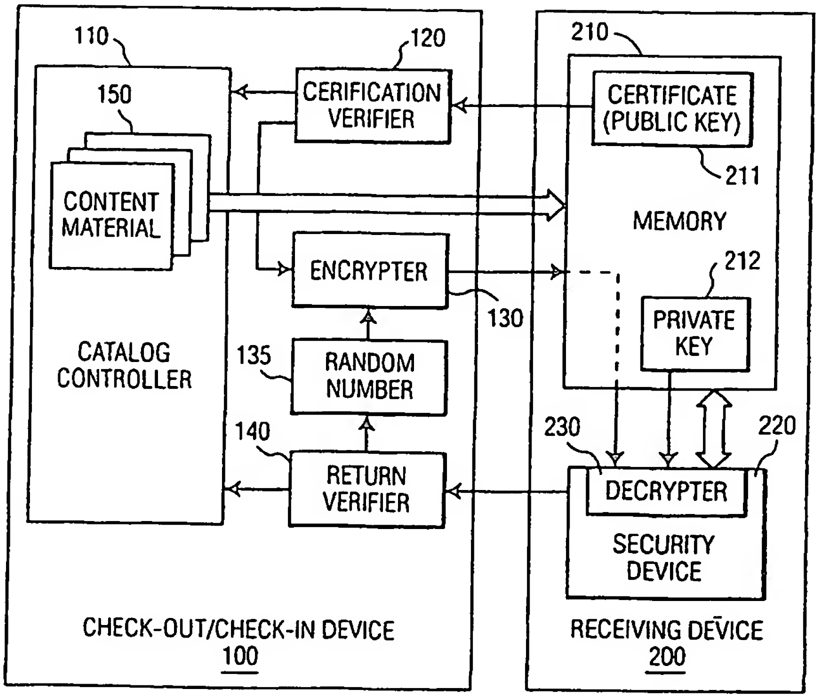
(81) Designated States: CN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: REGISTERING COPY PROTECTED MATERIAL IN A CHECK-OUT, CHECK-IN SYSTEM

(57) Abstract

In a limited-copy protection scheme, a check-out/check-in system is configured to a) verify that the receiving device is a certified conforming device, and b) verify that the device that checks-in content material is the same device that checked-out the content material. The verification of the receiving device is effected via a conventional certification process. The verification that the same device is used for check-in and check-out is effected via a secure challenge-response protocol. As contrast to a conventional contemporaneous challenge-response protocol, the system provides a challenge that is specific to the receiving device when the content material is checked-out, and verifies the appropriate response when the content material is checked-in. Because the challenge-response is specific to the receiving device, only the device that receives the challenge when the content material is checked-out can provide the appropriate response when the content material is checked-in.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

Registering copy protected material in a check-out. check-in system.

This invention relates to the field of consumer devices, and in particular to techniques for preventing or discouraging the illicit duplication of copy protected material.

Techniques are continually being proposed and developed to prevent or discourage the illicit duplication of copy-protected material, such as commercial music recordings. These techniques generally attempt to limit the number of copies that can be made from a legitimate copy of the copy-protected material. At the same time, the purchaser of this legitimate copy expects to have unlimited rights for copying this material for his or her private purposes. For example, the typical purchaser has access to multiple means for playing and recording the material, and expects to be able to play the purchased material on each of these means, without constraints.

Increasingly common in the art is the use of flash memory cards to record content material for playback on small portable devices. These flash memory cards, or similar electronic memory devices, have an advantage over conventional recording media such as discs or tapes, in that they contain no moving parts and are thus more reliable and robust. Similarly, the playback devices for these memory cards need not contain movement mechanisms and are therefore also more reliable, robust, and, in general, less expensive than conventional players. The electronic memory devices and corresponding players are also generally much smaller than conventional discs or tapes and corresponding players, and generally consume less power, further increasing their suitability for use as portable playback systems.

One method for limiting the ability to copy the content material is a "check-out/check-in" system. In this, as in other protection schemes presented herein, it is assumed that the copying and playback devices are "conforming" devices, in that they conform to the standards used to protect copy-protected material. When a copy of the material is made from a providing device to a portable medium, the conforming providing device prevents additional copies from being made until the portable medium containing the copy is returned to the providing device. That is. the check-out/check-in system provides a "one-at-a-time", or an "at-most-N-at-a-time". copy scheme to limit the number of simultaneously available copies of protected content material.

A check-out/check-in system is susceptible to a variety of attacks intended to overcome the security provided by a check-out/check-in system. The most straightforward attack is one in which a non-conforming device is used to receive the material. After receiving the material, the non-conforming device provides unlimited copies. Another attack is one in which a non-conforming device "checks-in" material that another device received. A conforming device can receive/check-out the material, the non-conforming can "check-in" the material, and another conforming device can then receive the material, because the check-out/check-in system believes that the other copy has been returned. In this manner, an unlimited number of copies can be made to conforming devices, such as the aforementioned flash memory cards.

It is an object of this invention to provide a reliable check-out/check-in system and method for limiting the number of copies of protected content material that are simultaneously available. It is a further object of this invention to provide a reliable system and method for assuring that protected content material is provided only to devices that conform to copy protection standards established for protecting the content material. It is a further object of this invention to provide a reliable system and method for assuring that the device that checks-out content material is the same device that checks-in the content material.

These objects and others are achieved by a check-out/check-in system that is configured to a) verify that the receiving device is a certified conforming device, and b) verify that the device that checks-in content material is the same device that checked-out the content material. The verification of the receiving device is effected via a conventional certification process. The verification that the same device is used for check-in and check-out is effected via a secure challenge-response protocol. As contrast to a conventional contemporaneous challenge-response protocol, the system provides a unique challenge that is specific to the receiving device when the content material is checked-out, and verifies the appropriate response when the content material is checked-in. Because the challenge-response is specific to the receiving device, only the device that receives the challenge when the content material is checked-out can provide the appropriate response when the content material is checked-in.

The invention is explained in further detail. and by way of example, with reference to the accompanying drawings wherein:

Fig. 1 illustrates an example block diagram of a check-out/check-in system in accordance with this invention.

Fig. 2 illustrates an example flow diagram of a check-out/check-in system in accordance with this invention.

Throughout the drawings, same reference numerals indicate similar or corresponding features or functions.

This invention is based on the premise that a reliable check-in/check-out system has two fundamental requirements. Such a system requires a reliable means of verifying that the receiving device is a certified conforming-device. Otherwise, the copy provided to a potentially non-conforming device may be illicitly reproduced, thereby obviating the copy protection provided by a check-out/check-in system. Additionally, the system requires a reliable means of verifying that the checked-in material is being returned from the same certified conforming-device that initially checked-out the material. Otherwise, a non-conforming device can be used to 'check-in' material that another device, including a conforming device, received. Other security techniques, common in the art, may also be applied, for increased copy and distribution protection.

Fig. 1 illustrates an example block diagram of a check-out/check-in system in accordance with this invention. The check-out/check-in system includes a check-out/check-in device 100 and a receiving device 200. The check-out/check-in device includes a catalog controller 110 that controls access to a catalog of content material 150 to certified receiving devices. The controller 110 limits the number of copies of each content material 150 that are simultaneously available. In a preferred embodiment, the controller 110 maintains a count of the number of copies of the content material 150 that have been provided to, or "checked-out" to, certified receiving devices, and refuses to provide additional copies when a pre-defined limit is reached. The check-out/check-in system allows a receiving device 200 to "return", or "check-in" a copy of the content material 150, so that it can be provided to another receiving device. The receiving device 200 is presumed to be a conforming device, and a "return" of the material 150 corresponds to a termination of access to the copy of the content material 150 by the receiving device 200, and the "return" is a notification to the check-out/check-in device 100 that the receiving device 200 has terminated the access. Upon receipt of the "return" notification, the check-out/check-in device 100 decrements the count of the number of copies of the content material 150 that have been provided to receiving devices, thereby allowing another copy of the content material 150 to be provided to a certified receiving device.

A conforming receiving device 200 includes a "certificate" 211 that is issued by a trusted authority to certify that the receiving device is a device that is configured to conform to standards that have been established to protect copy protected content material. This certificate 211 typically includes a public key of a public-private key pair that is associated with the receiving device 200, the identity of the receiving device, and a digital signature based on a private key that is associated with the trusted authority. The digital signature binds the identity of the receiving device to the public key to the public key of the receiving device. The receiving device 200 communicates this certificate 211 to a certification verifier 120 in the check-out/check-in device 100. The certification verifier 120 applies a public key associated with the trusted authority to verify a correspondence between the communicated public key and the identity and authenticity of the receiver by means of the digital signature in the certificate 211. Because only the trusted authority can be expected to provide a digital signature that can be verified by the trusted authority's public key, the proper verification of the digital signature is a certification that the receiving device 200 is an authorized recipient for protected content material.

When the certificate is verified, the catalog controller 110 provides/checks-out the selected content material 150 to the receiving device 200, provided that the selected content material 150 has not already been checked-out to the maximum number of simultaneous receivers, based on the count parameter discussed above. That is, for example, if the content material 150 is limited to a single-copy-at-a-time distribution, then the catalog controller 110 will check-out the content material 150 to the receiving device 200 if and only if no other receiving device has checked-out this content material 150 and has not yet returned it.

In accordance with this invention, when the catalog controller 110 provides the copy of the content material 150 to the receiving device 200, the catalog controller 110 also issues a secure "challenge" to the receiving device, using any of a number of challenge-response protocols. In the example embodiment, the challenge is an encryption of a random number 135, based on the aforementioned public key of the public-private key pair that is associated with the receiving device 200. The random number 135 is provided by any number of techniques common in the art, including a pseudo-random number generator, a selection from a list, and so on. As noted above, preferably the certificate 211 contains this public key, and the certification verifier 120 provides this certified public key to an encrypter 130 to effect the encryption of the random number 135. The receiving device 200 stores the challenge in its memory 210, along with the associated content material 150.

As in conventional transfer systems, the content material 150 is provided to the receiving device in a secure form. The content material 150 may be encrypted using the aforementioned public key of the receiving device, and subsequently decrypted by the receiving device using a decrypter 230 and the receiving device's corresponding private key 212. Alternatively, the content material 150 may be encrypted using a particular key, and this particular key is encrypted using the public key of the receiving device. The receiving device 200 decrypts the encrypted key using the private key 212, and uses the decrypted key to decrypt the content material 150. These and other techniques for communicating protected content material are common in the art.

When a user of the receiving device 200 decides to return/check-in the content material to the check-out/check-in device, to allow another device to receive a copy of the content material, the receiving device is placed in communication with the check-out/check-in device, and the check-in process is initiated. In accordance with this invention, when placed in a check-in state, a security device 220 in the receiving device 200 erases the selected content material 150 from its memory 210, or otherwise terminates access to this content material 150, and communicates a "response" to the aforementioned "challenge" that was received when the content material 150 was received. In the example embodiment, the decrypter 230 within the security device 220 decrypts the encrypted random number that was received, and communicates the decrypted random number to the return verifier 140 of the check-out/check-in device 100. The return verifier compares the received decrypted random number to the original random number 135 to verify that the receiving device 200 is the same device that received the content material 150. Note that because the receiving device is assumed to be the only device having access to the receiving device's private key 212, and the encryption of the random number 135, and the content material 150, is based on the receiving device's public key, only the receiving device can return a decrypted random number that matches the original random number 135.

As will be evident to one of ordinary skill in the art, the catalog controller will typically contain a variety of content material that can be checked-out, and will typically check-out selected content material to a variety of receiving devices. Not illustrated, the catalog controller 110 and/or the return verifier 140 will contain a list of each checked-out content material and the random number associated with each checked-out content material, to effectively manage the check-out/check-in process. In like manner, each content material may have a different limit to the number of copies that may be simultaneously provided, with some content material allowing an unlimited number of simultaneous copies, and the catalog controller 110 is configured to enforce each limit as required.

Fig. 2 illustrates an example flow diagram of a check-out/check-in system in accordance with this invention. At 310, the check-out/check-in device receives a transaction request that includes an identification of the content material, and a certificate that verifies that the receiving device is a conforming device. As discussed above, in a preferred embodiment, the certificate includes the public key of a public-private key pair that is associated with the receiving device. If, at 315, the certificate is determined to be invalid, the process is aborted; otherwise, the type of transaction is determined, at 325. If the transaction is a request to check-out content material, the current count of the number of copies of the requested content material is compared to the limit of the number of simultaneous copies permitted, at 335. If the number of currently checked-out copies is not less than the limit, the process is aborted. If the number of currently checked-out copies is less than the limit, a challenge is generated, at 340, and the challenge and the content material are transmitted to the receiving device, at 350. The current count of the number of checked-out copies is incremented, at 360, thereby corresponding to a check-out of the content material.

If, at 325, the transaction is a return/check-in of content material, the check-out/check-in device receives the response to the challenge that was given to the receiving device checked-out the content material, at 370. If the response is an appropriate response to the challenge, at 375, the current count of the number of checked-out copies of the content material is decremented, at 380, thereby corresponding to a "return" of the content material, and the process continues. If the response does not correspond to the challenge, at 375, the count is not decremented.

After incrementing or decrementing the count, or after aborting, the process continues at 390, typically by looping back to step 310, to await another transaction request. Note that the flow 310-325 can be modified to bypass the 're-certification' of the receiving device when content material is being returned, on the assumption that only a previously certified receiving device will be able to provide an appropriate response to the challenge, at 370.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within the spirit and scope of the following claims.

CLAIMS:

1. A method for limiting simultaneous copies of content material (150), comprising:

- communicating (350) a copy of the content material (150) to a receiving device (200),
- communicating (350) a security challenge to the receiving device (200) when the copy of the content material (150) is communicated to the receiving device (200), and-
- receiving (370) a security response, based on the security challenge, from the receiving device (200) when the copy of the content material (150) is removed from the receiving device (200).

2. The method of claim 1, further including

- verifying (315) a certification (211) of the receiving device (200) before communicating the copy of the content material (150) to the receiving device (200).

3.The method of claim 1, further including

- maintaining a count of the simultaneous copies of the content material (150), including:

incrementing (360) the count when the copy of the content material (150) is communicated to the receiving device (200), and

decrementing (380) the count when the security response is received from the receiving device (200),

- wherein
- communicating (350) the copy of the content material (150) is dependent upon the count of the simultaneous copies.

4. The method of claim 1, further including:

- generating (340) a random number, and
- encrypting (340) the random number via a public key of a public-private key pair that is associated with the receiving device (200) to form the security challenge, and
- wherein
- the security response includes the random number.

5. A check-out/check-in device (100) comprising:

- a catalog controller (110) that is configured to provide a limited number of simultaneous copies of content material (150) to one or more receiving devices,
- an encrypter (130) that is configured to provide a security challenge to a receiving device (200) of the one or more receiving devices when the catalog controller (110) provides a copy of the content material (150) to the receiving device (200), and
- a return verifier (140) that is configured to:

receive a security response from the receiving device (200) when the copy of the content material (150) is removed from the receiving device (200), and

notify the catalog controller (110) whether the security response corresponds to an appropriate response to the security challenge.

6. The check-out/check-in device (100) of claim 5, further including

a certification verifier (120) that is configured to verify a certification (211) of the receiving device (200),

- wherein
- the catalog controller (110) is further configured to provide the content material (150) in dependence upon the certification (211) of the receiving device (200).

7. The check-out/check-in device (100) of claim 5, wherein

- the catalog controller (110) is further configured to maintain a count of the simultaneous copies of the content material (150),
- wherein,
- the catalog controller (110) is configured to:

increment the count when the copy of the content material (150) is communicated to the receiving device (200), and

decrement the count when the security response is received from the receiving device (200), and

provide the copy of the content material (150) in dependence upon the count of the simultaneous copies.

8. The check-out/check-in device (100) of claim 5, wherein

- the encrypter (130) is configured to encrypt a random number via a public key of a public-private key pair that is associated with the receiving device (200) to form the security challenge, and
- the return verifier (140) is configured to compare the security response to the random number to determine whether the security response corresponds to the appropriate response to the security challenge.

9. A receiving device (200) that receives content material (150) and a corresponding security challenge from a check-out/check-in device (100), comprising:
- a memory (210) that is configured to store the content material (150) and the corresponding security challenge, and
- a security device (220) that is configured to:

  erase the content material (150) from the memory (210), and

  communicate a security response to the check-out/check-in device (100),

based on the security challenge that is associated with the content material (150).

10. The receiving device (200) of claim 9, wherein
- the security device (220) is further configured to communicate a certification (211) of the receiving device (200) to the check-out/check-in device (100) to enable the check-out/check-in device (100) to provide the content material (150) to the receiving device (200).

11. The receiving device (200) of claim 9, wherein
- the security device (220) includes:

  a decrypter (230) that decrypts the security challenge via a private key (212) of a public-private key pair that is associated with the receiving device (200) to form the security response.

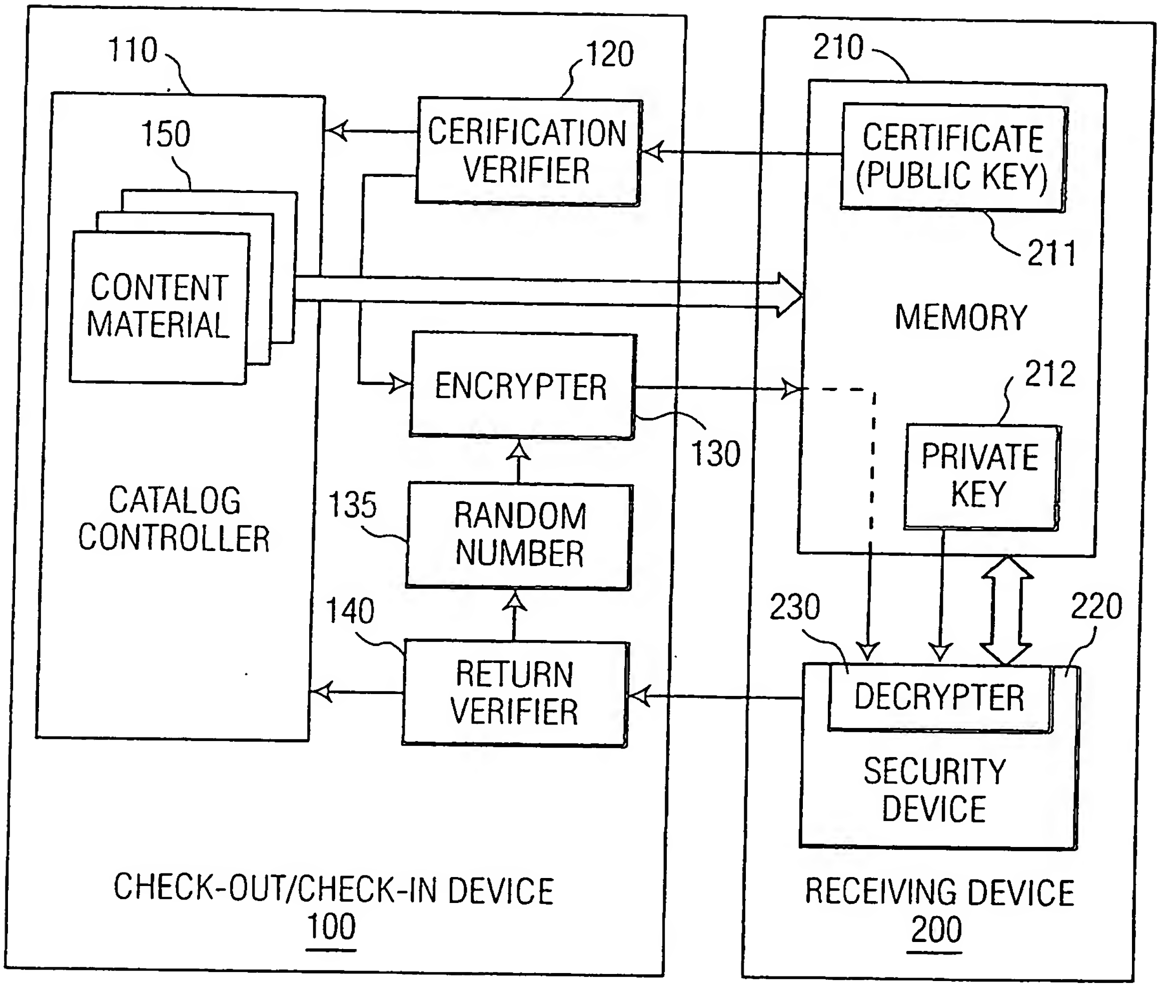

110
120
CERIFICATION VERIFIER
150
CONTENT MATERIAL
CATALOG CONTROLLER
ENCRYPTER
130
135
RANDOM NUMBER
140
RETURN VERIFIER
CHECK-OUT/CHECK-IN DEVICE
100
210
CERTIFICATE (PUBLIC KEY)
211
MEMORY
212
PRIVATE KEY
230
220
DECRYPTER
SECURITY DEVICE
RECEIVING DEVICE
200

FIG. 1

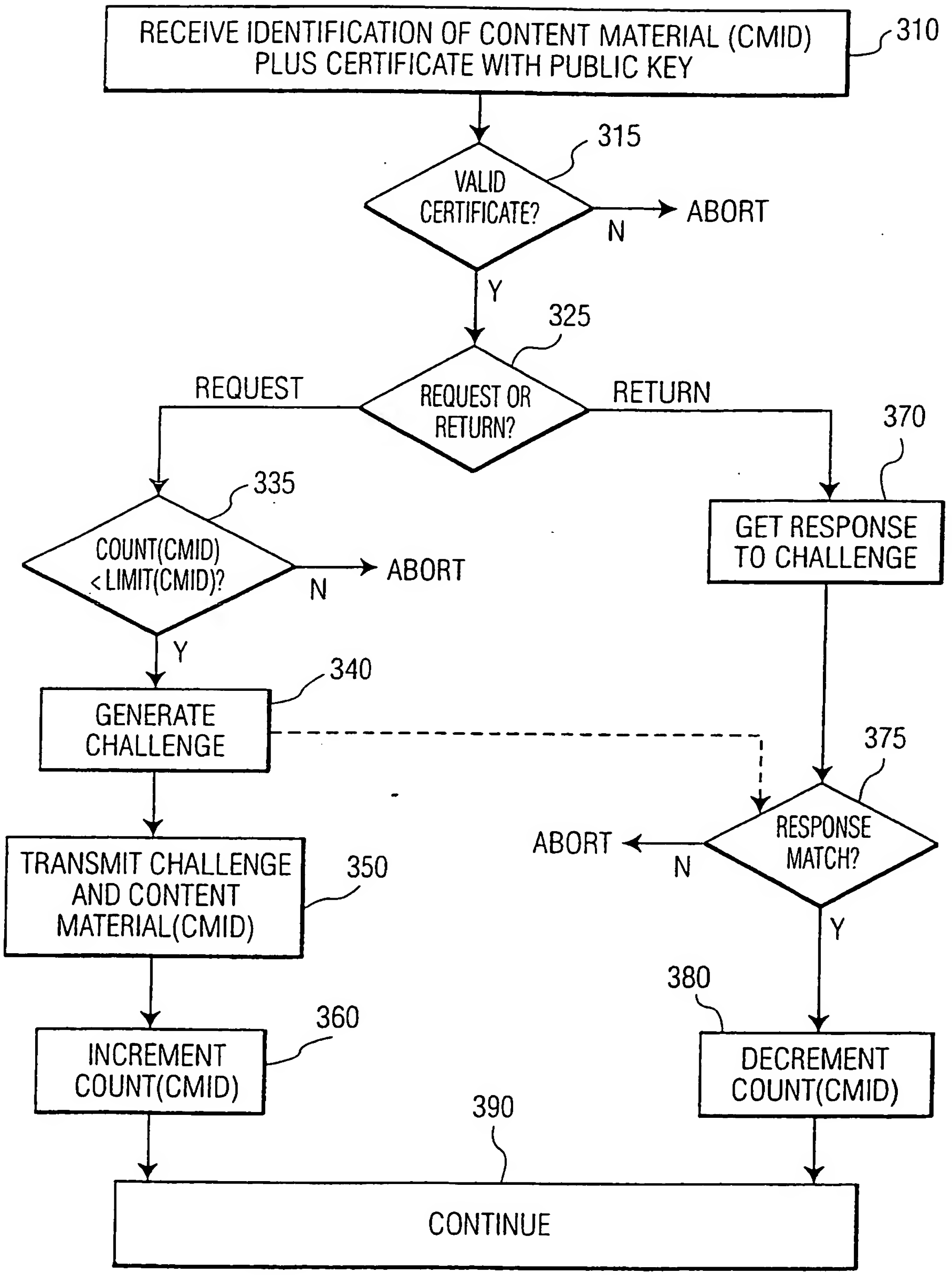

RECEIVE IDENTIFICATION OF CONTENT MATERIAL (CMID) PLUS CERTIFICATE WITH PUBLIC KEY
310
315
VALID CERTIFICATE?
N
ABORT
Y
325
REQUEST OR RETURN?
REQUEST
RETURN
335
COUNT(CMID) < LIMIT(CMID)?
N
ABORT
Y
340
GENERATE CHALLENGE
TRANSMIT CHALLENGE AND CONTENT MATERIAL(CMID)
350
INCREMENT COUNT(CMID)
360
370
GET RESPONSE TO CHALLENGE
375
RESPONSE MATCH?
N
ABORT
Y
380
DECREMENT COUNT(CMID)
390
CONTINUE

FIG. 2

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/EP 00/03801

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 390 297 A (BURKLEY RICHARD M ET AL) 14 February 1995 (1995-02-14)	1-3,9,10
A	abstract; figures 3,4 column 2, line 19 - line 54 column 3, line 42 -column 4, line 30 column 9, line 29 -column 12, line 5 figures 1-3 ---	5-7
A	EP 0 462 918 A (IBM) 27 December 1991 (1991-12-27) abstract column 2, line 53 -column 3, line 7 column 3, line 49 -column 4, line 56 column 5, line 57 -column 7, line 34 figures 1-3 --- -/--	1-3,5-7, 9

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 July 2000	Date of mailing of the international search report 03/08/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Schiwy-Rausch, G

INTERNATIONAL SEARCH REPORT

Inte ,ional Application No
PCT/EP 00/03801

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropnate, of the relevant passages	Relevant to claim No.
A,P	GB 2 343 025 A (IBM) 26 April 2000 (2000-04-26) abstract; figures 1,2 page 1, line 27 - line 43 page 5, line 4 - line 29 figures 1,2,5,8 ---	1-3,5-7
A	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 09, 31 July 1998 (1998-07-31) & JP 10 111797 A (NEC CORP), 28 April 1998 (1998-04-28) abstract ---	1,2
A	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 11, 30 September 1998 (1998-09-30) & JP 10 149283 A (FUJITSU LTD), 2 June 1998 (1998-06-02) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ›onal Application No
PCT/EP 00/03801

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5390297 A	14-02-1995	AU 618056 B	12-12-1991
		AU 2782289 A	01-06-1989
		CA 1310425 A	17-11-1992
		CN 1035192 A	30-08-1989
		EP 0355132 A	28-02-1990
		JP 2501171 T	19-04-1990
		WO 8904520 A	18-05-1989
EP 0462918 A	27-12-1991	US 5251315 A	05-10-1993
		JP 5151049 A	18-06-1993
GB 2343025 A	26-04-2000	NONE	
JP 10111797 A	28-04-1998	NONE	
JP 10149283 A	02-06-1998	NONE	